REMARKS

Claims 1-36 are pending Claims 1-36 are pending. Please amend claims 1-31 and 33-36. Kindly cancel claim 32 without prejudice. No claims are added. In view of the following remarks/arguments, withdrawal of all outstanding objections and rejections to the pending claims is respectfully requested.

35 USC §101 Rejections

Claims 1-10 stand rejected under 35 USC §101 as being directed to non-statutory subject matter. The Action asserts that claims 1-10 fail to produce a tangible result. Applicant respectfully disagrees. Claim 1 recites "form a logical model of the application", which is a tangible result. Additionally, claim 1 recites "to identify a set of potential security threats", which is also a tangible result. **Claims 2-10** depend from claim 1. Claims 1-10 do produce a tangible result.

Withdrawal of the 35 USC §101 rejection of claims 1-10 is requested.

Claim Rejections Under 35 USC §102(a)

Claims 1-36 stand rejected under 35 USC §102(a) as being anticipated by "Security Analysis & Design" by Uttara Nerurkar ("Nerurkar"). This rejection is traversed.

As a preliminary matter, Applicants response dated August 15, 2005 provided detailed reasons why Nerurkar does not anticipate the rejected claims. Those reasons are not reiterated verbatim herein, but are instead incorporated by reference. The Office is urged to review those reasons in view of the following remarks.

Claim 1 recites:

- A computer-implemented method for a computer-program module to provide application security threat-modeling, the method comprising:
    - providing class definitions for a plurality of model components to represent respective elements of an application, each model component specifying a set of security threat categories potentially applicable to the component ;
    - responsive to user input, interconnecting at least a subset of the model components to form a logical model of the application; and
    - automatically analyzing the at least a subset of model components and respective interconnections to identify a set of potential security threats corresponding to the at least a subset, the potential security threats being associated with one or more of the security threat categories.

In addressing Applicant's argument with respect to claim 1 that Nerurkar fails to describe computer-implemented method of any type, the Action supports its 35 USC 102 rejection of claim 1 by asserting that since Nerurkar "is an associate of the Software Concept Laboratory at Infosys Technologies Limited [,] is in and of itself, **sufficient to suggest** that the concept disclosed in the paper is in fact to be used in software, which is 'computer-implemented'" (emphasis added). Additionally, the Action asserts that since the Nerurkar article appeared in "Dr. Dobbs Software Tools for the Professional Programmer" [...] that the method disclosed would be programmed into a software by a professional programmer." Firstly, Applicant disagrees with these assertions. Secondly, in a rejection based

on 35 USC 102 it is irrelevant if Nerurkar is only "sufficient to suggest" a clearly missing claimed feature.

The standard in an anticipation rejection is not "sufficient to suggest" a missing feature. "Sufficient to suggest" is a question of obviousness. Rather, to provide a valid finding of anticipation, several conditions must be met:

(i) the reference must include every element of the claim within the four corners of the reference (see MPEP §2121);

(ii) the elements must be set forth as they are recited in the claim (see MPEP §2131);

(iii) the teachings of the reference cannot be modified (see MPEP §706.02, stating that "No question of obviousness is present" in conjunction with anticipation); and

(iv) the reference must enable the invention as recited in the claim (see MPEP §2121.01). Additionally, (v) these conditions must be simultaneously satisfied.

Since the Action supports a 35 USC 102 rejection of claim 1 by asserting that Nerurkar is only "sufficient to suggest" a feature required by claim 1,a feature that is clearly missing from Nerurkar, the Action has failed to present a prima facie case of anticipation of claim 1.

For this reason alone, withdrawal of the 35 USC §102 rejection of claim 1 is requested.

Moreover, Applicant respectfully submits that Nerurkar's techniques for threat analysis, irrespective of whether they rely on handwritten or computer generated documents, are completely silent on any teaching of "automatically

analyzing" such documents to identify " a set of potential security threats corresponding to the at least a subset, the potential security threats being associated with one or more of the security threat categories", as claim 1 requires. Nerurkar does not describe other features of claim 1 as well. For example, "providing class definitions for a plurality of model components to represent respective elements of an application, each model component specifying a set of security threat categories potentially applicable to the component", as claim 1 requires.

For these additional reasons, withdrawal of the 35 USC §102 rejection of claim 1 is requested.

Claims 2-10 depend from claim 1 and are not anticipated by Nerurkar solely based on this dependency. Additionally, claims 2-10 recite additional features that are not anticipated by Nerurkar.

For example, claim 5 recites "selecting a particular component of the model components", and "responsive to selecting the particular component, displaying each other component of the model components that comprise at least a subset of similar potential security threats as the particular component." In addressing this claimed feature, the Action asserts that it is described by Nerurkar's partition based on the similarity and nature of security concerns of the components (page 52, column 1, ¶ 3). Applicant disagrees. Nerurkar at page 52, column 1, ¶ 3, merely describes that "[t]he onion is now partitioned into peels based on the similarity in the nature and criticality of the security concerns of the components. [...] the peels are documented in the Peel Diagram." Clearly, this does not describe the something is selected or that anything is done in response to something being

selected. Thus, for these additional reasons, Nerurkar does not anticipate the features of claim 5.

In another example, claim 6 recites "selecting a particular component of the model components", and "responsive to selecting the particular component, displaying each other component of the model components that comprises a particular security threat similar to a security threat already addressed with respect to the particular component." In addressing this claimed feature, the Action asserts that it is described by Nerurkar's at page 52, column 2, ¶ 4). Applicant disagrees. Nerurkar at page 52, column 2, ¶ 4, merely defines an Internet User Interface Peel and describes placing network components in the Internet Communications Peel. The following paragraph of Nerurkar merely describes that because of interaction of an e-commerce application with a payment system, the Internet User Interface Peel should be divided into the Customer Interface Peel and Payment System Interface Peel. Clearly, nowhere do these explicit descriptions of Nerurkar teach that anything is done "responsive to selecting a particular component". For these additional reasons, Nerurkar does not anticipate claim 6.

Claim 11 recites:

- computer-executable instructions for providing application security threat-modeling, the computer-executable instructions comprising instructions for
    - defining a plurality of model components to represent respective elements of an application, each model component specifying a set of security threat categories potentially applicable to the component , the model components being defined with class definitions in a component schema;

- interconnecting, responsive to user input, at least a subset of the model components to form a logical model of the application; and
- analyzing the at least a subset and respective interconnections to identify a set of potential security threats associated with associated ones of the security threat categories.

For the reasons already discussed above with respect claim 1, Nerurkar does not anticipate these recited features.

Withdrawal of the 35 USC §102(a) rejection of claim 11 is requested.

Claims 12-20 depend from claim 11 and are not anticipated by Nerurkar solely in view of these respective dependencies. For this reason alone, withdrawal of the 35 USC §102(a) rejections of claims 12-20 is respectfully requested.

Claim 31 recites:

- a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for:
  - providing class definitions defining attributes of model components representing respective elements of an application, at least one attribute of the attributes associated with a model component specifying a set of security threat categories potentially applicable to the model component ;
  - presenting symbols associated with at least a subset of the model components on a display;
  - interconnecting respective ones of the at least a subset to form a logical model of the application; and

- analyzing the logical model in view of security threat categories associated with respective ones of the model components in the logical model to identify a set of potential security threats to the application.

For the reasons already discussed above with respect claim 1, Nerurkar does not anticipate these resided recited features.

Withdrawal of the 35 USC §102(a) rejection of claim 21 is requested.

Claims 22-30 depend from claim 21 and are not anticipated by Nerurkar solely in view of these respective dependencies.

Withdrawal of the 35 USC §102(a) rejections of claims 12-20 is requested.

Claim 31 recites:

- processing means for presenting a user interface for application security threat-modeling, the processing means comprising:
  - means for displaying and interconnecting a plurality of model components to design a logical model of an application, at least a subset of the model components comprising a corresponding set of potential security threat characteristics defined in a schema of class definitions for the model components;
  - means for specifying a component of the model components in the logical model;
  - means for identifying a set of potential security threats in view of one or more of module, port, store, or wire attributes associated with the at least a subset of model components that comprise the logical model; and
  - means for selecting a particular solution to mitigate the potential security threats in in the logical model.

For the reasons already discussed above with respect claim 1, Nerurkar does not anticipate these recited features. Additionally, Nerurkar is completely silent with respect to any such "schema".

Withdrawal of the 35 USC §102(a) rejection of claim 31 is requested.

Claims 32-36 depend from claim 31 and are not anticipated by Nerurkar solely in view of these respective dependencies. For this reason alone, withdrawal of the 35 USC §102(a) rejections of claims 32-36 is requested.

Conclusion

Claims 1-31 and 33-36 are in condition for allowance, and action to that end is respectfully requested. Should any issue remain that prevents allowance of the application, the Office is encouraged to contact the undersigned prior or issuance of a subsequent Office Action.

Respectfully Submitted,

Dated: 02/01/2006 By: Brian Hart

Brian G. Hart
Reg. No. 44, 421
(509) 324-9256